



DITCH THE PITCH

a guide for guarding against scams

A Publication from the SC Department of Consumer Affairs

table *of* contents

red flags.....	3
common scams.....	4
common digital scams.....	7
defend against other popular scams.....	10
defend against phone scams.....	12
important contact information.....	13
does a scammer have your information?.....	14

If it sounds too good to be true...

SCAM RED FLAGS

Below you will find a list of the most common signs of a scam. Look out for these red flags and you'll have a better chance of avoiding a scam. Be wary if someone:

- Asks you to verify personal identifying information.
- Asks you to wire transfer money or purchase a prepaid/reloadable debit card and give them the number off the card.
- Sends you a check, asking you to cash it and wire or send money somewhere.
- Poses as a local, state, or federal law enforcement officer. They may also pose as other government officials.
- Scares you with threats of arrest or garnishment.
- Makes you think their "offer" is time sensitive. ***"Act NOW, or you won't get this great deal!"***



Bottom Line: If you are fielding a cold call (email, text message, etc.) never give information to the person and when in doubt, **hang up and follow up!**

The more you know about scams, the less likely you are to be a victim of one. This guide outlines the anatomy of some of the most reported scams, so you can better avoid them!

c o m m o n scams


LOTTERY/SWEEPSTAKES


The Pitch: Scam artists will call or write saying you have won a lottery out of Australia, England or another foreign country. Some scammers use the names of well-known home improvement stores or super stores and allege you were entered into a drawing each time you shopped at the store and... you are a winner! In these scenarios, the scammer will ask you to wire or send money in order to receive your prize.

**“CONGRATULATIONS!
YOU’VE WON
\$250,000 IN
THE AUSTRALIAN
LOTTERY!”**

the defense

- Never send money to claim a prize, especially through a wire transfer. ***Wiring money to a location is like sending cash.***
- Don’t play along or engage with the scammer. It will only make them more likely to call you again.

 **RED FLAG:** Legitimate lotteries and sweepstakes will not ask you to pay a fee to collect your winnings.


 **RED FLAG:** Scam artists often say the up front fee is for “insurance,” “taxes,” “shipping and handling charges.”

FAKE DEBT COLLECTORS

The Pitch: The scammer, sometimes pretending to be from a state, federal or law enforcement agency, will try to get you to settle a debt you supposedly “owe.” The fraudster may ask you to pay a fraction of the amount, immediately, over the phone. In exchange, the debt will be forgiven. Some consumers have reported that the scammer had their personal information, making the call seem more legitimate. The “offer” to settle the debt is also made out to be time sensitive. If you don’t make the

payment right then, you will have to pay it all.

“YOU OWE \$5,000 IN CREDIT CARD DEBT, BUT WE’LL TAKE \$1,000 RIGHT NOW AS THE FINAL PAYMENT.”

 **RED FLAG:** The scammer threatens that you’ll be arrested if you don’t pay.

the defense


- Never give your credit card number or banking information to someone you do not know.
- Call the department the scammer posed as to let them know about the scam.
- Ask for something in writing from the “debt collector” so you can verify their claim. Federal law requires debt collectors to send you a letter about the debt.
- Check your credit report to see if the debt you “owe” is there. Get a free copy of your credit report @ www.annualcreditreport.com or by calling 877-322-8228.

IMPOSTERS

The Pitch: Fraudsters will pose as your bank and ask for personal or banking information needed to supposedly “verify” or “reactivate” your credit or debit account. The caller may claim that the information is needed to reverse a fraudulent charge or an error resulting in your card being blocked. The ruses for this type of scam are unlimited. Scammers also pose as government agencies like the IRS.

“YOUR GRANDSON IS IN TROUBLE AND NEEDS YOU TO WIRE HIM MONEY IMMEDIATELY!”

A different spin on the imposter scam has the scammer posing as a friend or a family member who is in trouble and needs money. The “trouble” often ranges from car problems to being in jail. Instead of your personal banking information, this time the caller wants you to wire money to assist your loved one.

 **RED FLAG:** The fraudster tells you not to tell anyone about the call/situation.

the defense

- Do not give your personal information or otherwise ‘verify’ your bank/credit card information over the phone.
- Hang up and dial your bank or credit card company directly and tell them about the call. Banks and credit unions will not phone you for this information.
- Before you send money to a caller insisting your family member or friend needs it, contact someone who could verify or debunk the story.

common digital scams

PHISHING

**“WE NEED TO
‘CONFIRM/UPDATE/
VERIFY’ YOUR ACCOUNT
INFORMATION.”**

Phishing is a scam where an Internet fraudster sends an e-mail that claims to be from a business you may have a relationship with. The message asks you to “confirm,” “update” or “verify” your personal information - for example your account number or social security number - or your online account user name or password. A website link for you to visit or telephone number for you to call may be included in the e-mail.

SMiSHING

SMiShing, similar to phishing, is an attempt to get personal information from you. The only difference is that SMiShing attempts come in the form of text messages instead of emails. The message may ask that you verify or update information, or it could contain a link with a virus or other malware that the scammer wants you to download onto your mobile device.

**“YOU’VE WON A FREE
\$100 GIFT CARD, JUST
CLICK [HERE](#) TO CLAIM!”**

the defense

- Do not reply to an e-mail, text or pop-up message that asks for personal or financial information.
- Do not click on any links in an email or text message or cut and paste the link into your browser.
- Do not call a phone number contained in the e-mail or text. If you are concerned and want to call the company, call a number you found in the phone book or by going to the company's website.
- Use antivirus or antispyware software and a firewall. Make sure to update them regularly. Phishing emails may contain software that can harm your computer or track your activities on the Internet.
- Always review your banking statements as soon as you receive them. Also review your credit report regularly. You are entitled to a free credit report from each one of the three major credit reporting agencies annually. You can get your report by visiting www.annualcreditreport.com or calling 877-322-8228. Check your statements and credit report for unauthorized purchases/accounts and incorrect information.



RED FLAG: Legitimate companies don't ask for this personal information via e-mail.

NOTE: Make sure you are on the look out for "spear" phishing attempts also. This is a spin on traditional phishing where scam artists have some inside information, such as your name or knowledge of who you do business with, which they use to seem more legitimate in their request for personal data.

AUCTION/AD SITES

Auction/Ad sites like eBay and Craigslist can be great tools for buying and selling. They are also hotbeds for scam activity. Scammers may offer to buy an item you've posted, but when you get the check you realize it's for a much larger amount than you asked. The scammer will tell you to cash the check, pay yourself and send the rest back to them.

**"CASH THIS CHECK
FOR \$1,250 AND WIRE
\$1,000 TO BILOXI."**

the defense

- There is never a valid reason to cash a check for someone and send the money back.
- Try selling to someone in your area. If you can't, talk to the buyer via phone.
- Be wary of a check for a larger amount than expected.
- Report the person to the site you are using.
- Request a check drawn on a local bank so you can make sure it is valid.



RED FLAG: Look out for spelling and grammar errors in e-mails.



defend against *other popular* **scams**

SECRET SHOPPER

- Steer clear of offers that come through the mail with a check included.
- Look for a legitimate secret shopper job through the Mystery Shopper Providers Organization of North America by visiting mspa-na.org.
- Never cash a check from someone you don't know and wire the money.

JURY DUTY

- Information about jury duty will come through the mail, not a phone call.
- Courts and law enforcement officers will not call or email you asking for personal information or money.
- Don't trust your caller ID; scammers can easily spoof their phone number to look like it is a local call.

HOME REPAIR

- Do not pay in full upfront.
- Make sure all details are in a written contract and you get a completed copy.
- Check with the SC Department of Labor Licensing and Regulation at www.llr.state.sc.us to verify licensure.

FAKE CHARITIES

- The Secretary of State's Office has a list of good and bad charities. Call 803-734-1790 or visit www.scsos.com for a copy.
- Avoid charities soliciting door-to-door.
- Stick with recognized charities that are well-established.
- Ask any cold caller to send you information about the charity through the mail.

HEALTH FRAUD

- Be aware of false ads for free medical services or products.
- Medicare and Medicaid will never call and request your personal information over the phone.
- If called, do not agree to enroll in health insurance plans over the phone. Ask for information in writing.

SHAM INVESTMENTS

- Legitimate offers will not disappear overnight. Do not feel pressured to make a quick decision.
- Involve a family member or professional when a stranger promises a large profit on an investment.
- Think twice if you are told "your profit is guaranteed" or "there is no risk."

3 **ways** **TO DEFEND** *against phone* **scams**

**1. Don't fall for
high pressure tactics**



**2. Be suspicious of wire
transfer or reloadable debit
card payment requests**



**3. When in doubt,
hang up and follow up**

important contact information

REPORT SCAMS TO:

SCDCA: 800-922-1594 or www.consumer.sc.gov

FTC: 877-382-4357 or ftccomplaintassistant.gov

FCC: 888-225-5322 or fcc.gov/complaints (phone)

DO NOT CALL REGISTRY

Add your number to the Do Not Call Registry:

Donotcall.gov or 888-382-1222

STOP UNSOLICITED OFFERS

Opt out of snail mail marketing:

Dmchoice.org

Opt out of preapproved credit offers:

www.optoutprescreen.com or call 888-567-8688.

FREE CREDIT REPORT

Get a copy of your FREE credit report:

www.annualcreditreport.com or call 877-322-8228.

does a scammer *have your* information?

If you have shared your information with a scammer, there are some steps you should take to minimize the damage!

STEP #1: FRAUD ALERT

Place a Fraud Alert: Its FREE, stays in place for 90 days and requires a business to take steps to verify that it is in fact you that is applying for the good or service. Call one of the credit bureaus and they'll notify the other two.

STEP #2: SECURITY FREEZE

Consider a Security Freeze: Its FREE and will prevent a business from accessing your credit report for new products or services, unless you temporarily lift the freeze. You must call each of the credit bureaus to do this.

Equifax: 800-685-1111

TransUnion: 800-680-7289

Experian: 888-397-3792

You can use these numbers for both the fraud alert and the security freeze.

STEP #3: MONITOR

Monitor Financial and Personal Statements: Be sure that your bills and statements are arriving on time and are correct. ID Thieves don't just use your information to get money. Your SSN can be used to receive:

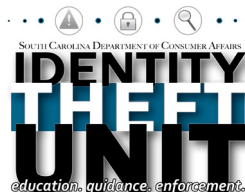
- Government benefits
- Driver's License/ID
- Tax refund
- Medical benefits

So, be sure to monitor **ALL** of your statements, and always be on alert for any suspicious or unexpected letters or phone calls!

FOR ADDITIONAL HELP:

Contact the South Carolina Department of Consumer Affairs' ID Theft Unit for more tips on dealing with identity theft and scams.

800-922-1594 • www.consumer.sc.gov



Check out our
YouTube channel.
youtube.com/scdcatv



Find the latest scam
alerts and news here.
twitter.com/scdca



Look here for updates &
educational materials.
facebook.com/scdca



South Carolina Department of Consumer Affairs
2221 Devine St. STE 200 • PO Box 5757 • Columbia, SC 29250
800-922-1594 • www.consumer.sc.gov

- JUNE 2015 -